Global Survey Finds More Than One Third of Companies Believe Their Intellectual Property Has Been Stolen

July 7, 2010 2:47 AM ET

*While Snooping Continues to Rise, IT Security Is Making It Harder for Insiders to Get Around Controls That Protect Highly-Sensitive Information*NEWTON, Mass. and LONDON - July 7, 2010 - The Results of Cyber-ArkÂ® Software's fourth annual "Trust, Security and Passwords" global survey show that 35 percent of respondents believe their company's highly-sensitive information has been handed over to competitors. Thirty-seven percent of the IT professionals surveyed cited ex-employees as the most likely source of this abuse of trust. While perhaps not surprising that disgruntled workers top the list, it's noteworthy that 28 percent suspected "human error" as the next most likely cause, followed by falling victim to an external hack or loss of a mobile device/laptop, each at 10 percent. The most popular information shared with competitors was the customer database (26 percent) and R&D plans (13 percent).Cyber-Ark's fourth annual "Trust, Security and Passwords" global survey is the result of interviews conducted in the Spring of 2010 with more than 400 senior IT professionals both in the US and UK, mainly from enterprise-class companies.There was little year-over-year change in the number of respondents who suspected the loss of intellectual property to a competitor, indicating that more needs to be done to protect companies' most valued assets. Additionally, to address vulnerabilities related to human error that could expose a proprietary database or financial information, organizations must employ additional layers of control such as the ability to grant privileges to sensitive data and systems on-demand. This limits "innocent" mistakes by allowing access to information only when users need it to perform a particular task or query.Snooping On the Rise, but Access Is Getting More DifficultThe research also confirmed that snooping continues to rise within organizations both in the UK and the US. Forty-one percent of respondents confessed to abusing administrative passwords to snoop on sensitive or confidential information â€“ an increase from 33 percent in both 2008 and 2009. When examining the information that people were willing to circumvent the rules to access, US respondents targeted the customer database first (38 percent versus 16 percent in the UK) with HR records most alluring to UK respondents (30 percent versus 28 percent in the US).Despite the rise, there was also the admission that organizations are trying to better curb snooping and are installing stronger controls to prevent these incidents. Based on this year's survey, 61 percent responded they could circumvent those controls â€“ a decrease from 77 percent in 2009. Additionally, 88 percent of IT professionals believe their use of these privileged accounts should be monitored, however only 70 percent of organizations actually attempt to do so â€“ with one-third turning a blind eye to what's happening within their networks and therefore failing to meet regulatory and compliance requirements. Insider sabotage, unfortunately and rather disconcertingly, has increased from 20 percent last year to 27 percent this year.Speaking about the results, Cyber-Ark's Executive Vice President Americas and Corporate Development Adam Bosnian commented, "While we understand that human nature and the desire to snoop may never be something we can totally control, we should take heart that fewer are finding it easy to do so, demonstrating that there are increasingly effective controls available to better manage and monitor privileged access rights within organizations. With insider sabotage on the increase, the time to take action has already passed and companies need to heed the warnings.""It is the organization's obligation to protect its sensitive information and intellectual property. Failing to do so, in our opinion, makes the company as bad as those who are abusing their privileged positions. Let's face it, you might as well sell the information to the highest bidder yourself â€“ that way at least youâ€™ll have some control over whoâ€™s got it!," continued Bosnian.IT Confess to Being the Best at SnoopingThe survey found that 67 percent of respondents admitted having accessed information that was not relevant to their role. When asked what department was more likely to snoop and look at confidential information, more than half (54 percent) identified the IT department, likely a natural choice given the group's power and broad responsibility for managing multiple systems across the organization. Of note, this is an up-tick compared to the 35 percent who identified the IT department as likely suspects in 2009, a number that had decreased from 47 percent in 2008. Respondents identified Human Resources the next curious at 11 percent, followed by administrative assistants.Note to editors:This survey was conducted with more than 400 IT administrators at Infosecurity Europe 2010 and RSA USA 2010. To download a detailed report of the survey results, please visit http://www.cyberark.com/constants/white-papers.asp.**About Cyber-Ark**Cyber-ArkÂ® Software is a global information security company that specializes in protecting and managing privileged users, applications and highly-sensitive information to improve compliance, productivity and protect organizations against insider threats. With its award-winning Privileged Identity Management (PIM) and Highly-Sensitive Information Management software,

organizations can more effectively manage and govern application access while demonstrating returns on security investments. Cyber-Ark works with more than 650 global customers, including more than 35 percent of the Fortune 50. Headquartered in Newton, Mass., Cyber-Ark has offices and authorized partners in North America, Europe and Asia Pacific. For more information, visit www.cyberark.com.

Wednesday, July 7, 2010 - 13:45